GUIDE 2025/2026

EU AI Act guide for mid-sized companies

AI compliance, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is the EU AI Act? 3

1.1 The regulation in plain words 3

1.2 The four risk classes 3

1.3 The timetable 4

1.4 How it sits alongside other rules 4

2 Are you in scope? 6

3 The road to compliance — seven phases 8

4 What does AI Act compliance cost? 10

5 The ten most common mistakes 12

6 Readiness check: are you ready? 14

7 Glossary 16

8 Your next step 18

1 What is the EU AI Act?

1.1 The regulation in plain words

The **EU AI Act** (Regulation (EU) 2024/1689) is the world's first comprehensive law regulating artificial intelligence. It came into force on **1 August 2024** and becomes binding EU-wide in stages. The aim: to make sure AI systems in the EU are trustworthy, transparent and under human control.

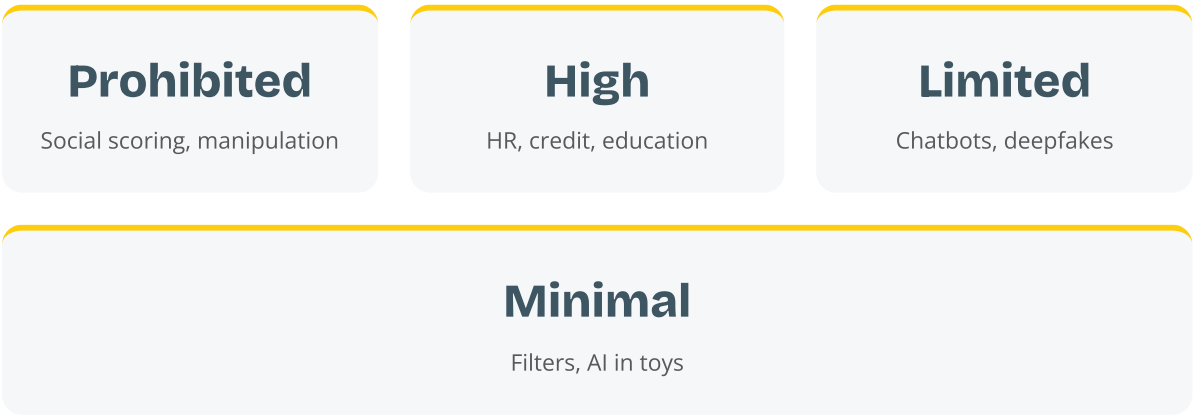
Unlike data protection law, the AI Act regulates **AI systems** , not data. It takes a **risk-based approach**: the higher the risk of an application, the stricter the duties. Social scoring systems, for instance, are prohibited; high-risk AI — in HR, say — has to be registered, documented and conformant.

> **The core idea:** the AI Act does not ask "do you use AI?" but "what risks does your AI pose to people — and how do you make sure those risks are controlled?"

The sanctions bite: up to **€35 million or 7 %** of worldwide annual turnover for prohibited practices. Up to **€15 million or 3 %** for breaching the high-risk duties. Up to **€7.5 million or 1 %** for supplying incorrect information to authorities.

1.2 The four risk classes

The AI Act sorts AI systems into four levels of risk:



1. **Unacceptable risk (Art. 5)** — prohibited. Examples: social scoring by public authorities, manipulative subliminal techniques, emotion recognition in the workplace, building facial databases by untargeted scraping of the internet.
2. **High risk (Art. 6 + Annex III)** — tightly regulated. Examples: AI in recruitment, lending, educational assessment, critical infrastructure, law enforcement, biometric

identification and medical diagnostics.

3. **Limited risk (Art. 50)** — transparency duties. Examples: chatbots (users have to know they are talking to AI), deepfakes (which have to be labelled) and AI-generated content.
4. **Minimal risk** — no duties. Examples: AI spam filters, AI in video games, simple recommendation algorithms.

> **An easy way to remember it:** the vast majority of everyday AI applications fall under minimal or limited risk. For a mid-sized company using standard tools — ChatGPT, Copilot, marketing software — usually only the Art. 50 transparency duties and the Art. 4 AI literacy duty apply.

1.3 The timetable

The AI Act applies in stages:

Date	What applies
2 February 2025	The Art. 5 prohibitions apply · the Art. 4 AI literacy duty is live
2 August 2025	The authorities' governance structure · the duties for general-purpose AI
2 August 2026	Duties for high-risk AI under Annex III · the Art. 50 transparency duties
2 August 2027	High-risk AI covered by existing sectoral EU legislation (Annex I)

1.4 How it sits alongside other rules

Rules	Focus	Relationship to the AI Act
EU AI Act	AI systems	The base regulation for AI
GDPR	Personal data	Complementary — AI using personal data falls under both
ISO 42001	AI management system	A voluntary ISO standard — evidence towards AI Act conformity

Rules	Focus	Relationship to the AI Act
Product liability (EU Dir. 2024/2853)	Liability for harm caused by AI	Complementary
Sectoral law (medical devices, machinery and so on)	Sector-specific	Remains in place, integrated with the AI Act

Worth knowing: ISO 42001 is the recommended standard for evidencing AI governance. If you are certified to it, you meet large parts of the high-risk duties automatically.

2 Are you in scope?

The AI Act applies EU-wide to providers and deployers of AI systems. Your duties depend on your **role** and on the **risk class** of the AI you use.

A. Your role under the AI Act

- **Provider:** you develop AI systems, or have them developed, and place them on the market or put them into service under your own name. The strictest duties.
- **Deployer:** you use AI systems in your own company — ChatGPT in support, for example. Lighter duties.
- **Importer:** you bring AI into the EU from a third country.
- **Distributor:** you resell AI systems.
- **Authorised representative:** you represent a third-country provider in the EU.

> **Important:** most mid-sized companies are deployers. They use finished AI products — ChatGPT, Microsoft Copilot, HR tools with AI features — while the AI itself is developed by the manufacturer.

B. Which duties apply, by role and risk class

Duties as a deployer — the most common case

- **AI literacy (Art. 4):** in force since 2 February 2025. Staff using AI need adequate knowledge, and it has to be documented.
- **Transparency (Art. 50):** chatbots have to be labelled as such, AI-generated images, video and audio have to be marked, and emotion recognition has to be disclosed.
- **Using high-risk AI:** with high-risk AI — a recruitment screening tool, say — you need human oversight, monitoring of use, and documentation.
- **A fundamental rights impact assessment** (for public bodies and certain high-risk applications).

Duties as a provider

- **A risk management system** across the whole lifecycle
- **Data governance**: training, validation and test data checked for quality
- **Technical documentation** evidencing conformity
- **Logging** of events automatically during use
- **Transparency and information** for deployers

- **Human oversight** by design
- **Accuracy, robustness and cybersecurity**
- **A quality management system**
- **Conformity assessment** and CE marking, for high-risk systems
- **Registration in the EU database** (for high-risk systems)

> *A real example: a marketing agency uses ChatGPT to write copy and Midjourney to generate images. It is a deployer. Its duties: AI literacy training for everyone using AI, and labelling any published AI-generated content under Art. 50.*

C. AI literacy (Art. 4) — the duty that applies most often

Every company using AI has to make sure its staff understand the technology. That means:

- A basic grasp of how AI works
- Awareness of the risks: bias, hallucination, data protection
- Knowing how to handle AI output — checking it critically rather than trusting it blindly
- Awareness of the legal framework

The effort is modest: a basic course of two or three hours per person, with attendance recorded, is usually enough.

3 The road to compliance — seven phases

For standard use of AI at limited risk, implementation is achievable in **four to eight weeks** . For high-risk AI, allow **four to eight months**.

1 **Build an inventory of AI systems**

Which AI systems are in use, and who is responsible for them? Staff tools often sit in shadow IT — private ChatGPT accounts, Copilot. Recording them systematically is the foundation. One to two weeks.

2 **Classify the risk of each system**

For each system: prohibited, high, limited or minimal, with the reasoning written down. The result is a risk matrix with the concrete duties per system. One to two weeks.

3 **An AI literacy programme**

Develop a basic course for everyone using AI, with more depth for power users in development, HR and marketing. Record attendance and refresh it yearly. Two to four weeks.

4 **Implement the transparency duties**

Label chatbots as AI. Mark AI-generated content in external communication. Disclose emotion recognition. Adjust the website, the marketing material and the products. Two to three weeks.

5 **Policies and rules**

An internal AI usage policy: which tools are allowed and which are not, what data may go into a prompt, who is responsible, what standards apply to prompting. Two to three weeks.

6 **For high-risk AI: additional measures**

Design the human oversight. Switch logging on. Carry out the fundamental rights impact assessment. Check the provider's conformity assessment. Set up monitoring. Six to twelve weeks.

7 **Governance and monitoring**

Appoint an AI officer. Review regularly, at least yearly. Watch what is new in AI and what needs documenting afterwards. Handle incidents when the AI

> misbehaves. Ongoing.

> **Tip:** Start with AI literacy and transparency — that satisfies the duties that apply most often, and takes four to six weeks. The demanding high-risk duties affect only a few companies; where they do, combine the work with ISO 42001.

4 What does AI Act compliance cost?

Costs vary a lot with the number of AI systems and with your role — deployer or provider of high-risk AI. Typical ranges:

Number of AI systems	Total cost*	Timeframe	Internal effort
1–2 systems (limited risk)	**€5,900–7,900**	3–5 weeks	5–10 hrs/week
3–5 systems	**€7,900–11,000**	4–6 weeks	7–12 hrs/week
6–10 systems	**€11,000–15,500**	5–7 weeks	10–16 hrs/week
11–25 systems	**€15,500–22,000**	6–9 weeks	14–22 hrs/week
25+ systems / provider of high-risk AI	**€22,000–34,000**	3–6 months	½-1 FTE

* Includes the inventory, risk classification, the AI literacy programme, implementing transparency and writing the policies. **Excludes** CE conformity assessment for high-risk AI of your own (a further €8,900–25,000 per system).

What drives the cost?

- **Your role:** a provider of high-risk AI faces far heavier duties than a deployer of limited-risk AI.
- **How many AI systems you have:** the more systems, the more work the inventory and the individual classification.
- **Your industry:** HR, lending, medicine and education run into the high-risk class more often.
- **An existing ISMS (ISO 27001):** cuts the documentation effort by 30 to 40 %.
- **Combining with ISO 42001:** saves 20 to 40 % against doing each separately, because many measures serve both.

Running costs

- The annual AI literacy refresher: around €2,000–4,000
- An external AI officer (optional): from €499 a month

- Conformity assessment of new high-risk systems: from €8,900 each
- Monitoring and incident response: around 20 to 30 % of the implementation cost per year

> **In the interest of transparency:** the AI Act is so new that market prices still vary widely. Others often quote €50,000–200,000 for a mid-sized project. Our approach, with template-based risk classification tools and ready AI literacy curricula, saves considerably at the same level of legal certainty.

5 The ten most common mistakes

1. **“We do not do AI”**
   Wrong. Anyone using ChatGPT, Copilot, HR tools with AI features, image generators or AI translation is a deployer within the meaning of the act. The literacy duty applies.

2. **Ignoring AI literacy**
   Mandatory since February 2025. Without documented training for everyone using AI you risk a fine — even with a single system.

3. **Not capturing shadow AI**
   Staff use private ChatGPT accounts for work and the company knows nothing about it. In an audit there is no dodging it.

4. **Classifying too quickly**
   “It is all limited risk”, without checking each case. An HR tool that screens applicants with AI, for instance, is high-risk.

5. **Ignoring the transparency duties**
   A chatbot on the website with no notice that the user is talking to AI. A complaint brings the risk of a fine.

6. **No AI usage policy**
   Staff put customer data into ChatGPT — a data protection problem and a compliance gap. The policy is the foundation.

7. **High-risk AI without human oversight**
   “The AI decides and we spot-check” is not enough. A human in the loop is mandatory.

8. **Not joining up the GDPR and the AI Act**
   AI systems usually process personal data — the two sets of rules have to be thought through together.

9. **Underestimating general-purpose models**

General-purpose AI has duties of its own from 2 August 2025. Training above 10^25 FLOPs brings further duties for systemic risk.

10 **Misjudging the timetable**

“The AI Act only applies from 2026” holds only for high-risk AI. The prohibitions, AI literacy and the general-purpose duties bite in 2025.

6 Readiness check: are you ready?

1. **Do you have a complete inventory of every AI system in the company?**
   Including the tools your staff use themselves — ChatGPT, Copilot and the like.
2. **Is every system classified against the AI Act risk classes?**
   Prohibited, high, limited or minimal — with the reasoning documented.
3. **Have the staff who use AI had literacy training?**
   Art. 4 — mandatory since 2 February 2025.
4. **Is there an internal AI usage policy?**
   Which tools, which data, who is responsible.
5. **Are chatbots and AI agents on your website labelled as such?**
   The Art. 50 transparency duty.
6. **Is AI-generated content — images, text — marked in external communication?**
   The labelling duty for deepfakes and AI content.
7. **For high-risk AI: is human oversight in place?**
   A human in the loop for the decisions that matter.
8. **Have you appointed an AI officer?**
   Responsible in practice for AI governance.
9. **Do you join up the AI Act with the GDPR?**
   The privacy policy, and an impact assessment where AI does the processing.
10. **Do you review your AI systems regularly for changes?**
    Yearly, or whenever something substantial changes.

Your yes answers	Assessment	Recommendation
0–3 × yes	**Act now**	A starting package: the inventory and AI literacy. Four to six weeks.
4–6 × yes	**The basics are there**	Focus on the gaps, above all transparency and the policies. Three to five weeks.

Your yes answers	Assessment	Recommendation
7–10 × yes	**Well positioned**	Fine-tuning and an annual review. Day-to-day operation is running.

7 Glossary

EU AI Act

Regulation (EU) 2024/1689 on artificial intelligence — in force since 1 August 2024.

AI system

A machine-based system with varying degrees of autonomy that generates outputs from inputs (Art. 3(1)).

Provider

Whoever develops an AI system or places it on the market. The strictest duties where the risk is high.

Deployer

Whoever uses an AI system. The typical role for a mid-sized company using ChatGPT, Copilot and the like.

Risk classes

Prohibited, high, limited, minimal — four levels with different duties.

Art. 4 (AI literacy)

The duty to ensure staff using AI have adequate knowledge. In force since 2 February 2025.

Art. 5 (prohibitions)

Prohibited practices: social scoring, manipulative subliminal techniques and others.

Art. 6 + Annex III (high risk)

The list of AI applications classified as high-risk.

Art. 50 (transparency)

The labelling duties for chatbots, deepfakes, AI content and emotion recognition.

GPAI (general-purpose AI)

General-purpose models such as GPT, Gemini and Claude. Duties of their own from August 2025.

Foundation Model

A large AI model adaptable to many purposes. Systemic risk applies above 10^25 FLOPs.

Human-in-the-Loop

Human oversight of AI decisions. Mandatory for high-risk AI.

Conformity assessment

The procedure for checking whether a high-risk AI system meets the requirements.

CE marking

The mark of conformity with EU law. Mandatory for high-risk AI.

EU database

The central register of high-risk AI systems. Providers have to register.

Notified Body

A conformity assessment body accredited at EU level.

Fundamental rights impact assessment (FRIA)

Mandatory for certain high-risk applications, particularly in the public sector.

8 Your next step

You have read this guide — that is the first step already. Tackling AI Act compliance in a structured way protects you from fines, builds trust in how you use AI, and gives you an advantage over more hesitant competitors.

A free first conversation

In 30 minutes, with no obligation, we work out together:

- ✓ Which AI systems are you already using?
- ✓ Which risk class applies?
- ✓ Which duties fall on you specifically?
- ✓ What budget and timeframe are realistic?

No sales pitch, no pressure — just an honest assessment.

> **The quick EU AI Act check**
> At **iso-easy.de** you can check in three minutes whether the act applies to you and which duties follow — without giving any contact details.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and compliance we support mid-sized companies in implementing the EU AI Act, ISO 42001, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.